UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

In re LastPass Data Security Incident Litigation	**Case Number: 1:22-cv-12047-PBS** **Hon. Patti B. Saris**

PLAINTIFFS' RESPONSE IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

SHAPIRO HABER & URMY LLP

Edward F. Haber (BBO# 215620)
Ian McLoughlin (BBO #647203)
Patrick J. Vallely (BBO# 663866)
One Boston Place, Suite 2600
Boston, Massachusetts 02108

Interim Liaison Counsel

Additional Interim Counsel for the Plaintiffs Listed on Last Page

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules and Other Authorities

INTRODUCTION

Defendants LastPass and GoTo are in the data security business. Plaintiffs are security-conscious individuals and businesses that trusted Defendants to protect their most sensitive and personal information. Defendants promised that their cutting-edge security technology would keep Plaintiffs' data safe. But Defendants broke their explicit data security promises resulting in a catastrophic data breach. Following this massive breach, Defendants have consistently minimized the impact of the breach and refused to accept responsibility for it—both in public statements to customers and now in their arguments to this Court. These arguments fail.

Defendants do not dispute that cybercriminals were able to steal copies of customers' entire LastPass "vaults," containing colossal amounts of data belonging to more than 25 million customers, including Plaintiffs. *See* Defendants' Memorandum in Support of Defendants' Motion to Dismiss, ECF No. 92-1 (hereafter "MTD"), at 14. Instead, Defendants claim that because customer vaults were encrypted, Plaintiffs' and Class members' "sensitive data was unimpacted" by the security breach. *Id.* at 15. But Plaintiffs allege that Defendants failed to implement industry-standard data security, that their personal and sensitive information was exfiltrated, and that cybercriminals were able to access the stolen vaults *and* decrypt data. Indeed, Defendants themselves have acknowledged that Plaintiffs are susceptible to "brute force" and phishing attacks from threat actors with limitless time to crack the stolen vaults in their possession. ¶¶ 276, 354.[1] Customers, including those with older master passwords, cannot protect themselves by changing passwords now, because the offline copies of the stolen LastPass vaults are protected by the stale passwords that were active when the vaults were stolen. ¶ 276. And, indeed, many customers have suffered significant damages from and losses as a direct result of this breach. *See generally* ¶¶ 11-230.

[1] Unless otherwise indicated, citations to the Consolidated Class Action Complaint (ECF No. 86, hereinafter "Complaint" or "CAC") are referenced herein as "¶ _" or "¶¶ __."

Worse, Defendants have withheld basic information about the data breach from both their customers and seemingly from regulators and state authorities. Defendants' pattern of obfuscation only leaves Plaintiffs and Class members in the dark, unable to adequately protect themselves from the consequences of the data breach. Instead of helping them, Defendants now seek dismissal of the Complaint to avoid meaningful discovery into the matter. Inverting applicable legal standards, Defendants ask this Court to simply take them at their word. But Plaintiffs plead cognizable injuries and allege sufficient facts to allow for the plausible and reasonable inference that Defendants' failure to safeguard Plaintiffs' and Class members' private information resulted in actionable damages. The Court should therefore deny Defendants' motion in its entirety.

STATEMENT OF FACTS

Defendants marketed and sold data privacy services with the explicit promise to customers that their "first priority" is "safeguarding your data . . . with proactive security." ¶¶ 3, 4, 6, 7, 270. LastPass even warned potential customers that "[d]ata breaches are on the rise" and "password security has never been more critical for individuals and businesses." ¶ 258. In an increasingly online world, LastPass claimed it is "almost impossible to keep your information safe without the help of an online vault" (coincidentally, a product that Defendants offered) and "[d]oing nothing could mean losing everything." ¶ 245. LastPass consistently encouraged potential customers to employ its "password vault" service, which LastPass explicitly described as "like a physical safe but for your online valuables" that would provide "peace of mind everywhere you go." ¶¶ 245, 259.

Relying on this illusion of security, Plaintiffs and Class members entrusted LastPass with their most sensitive and personal information. ¶¶ 20, 33, 47, 62, 75, 91, 101, 112, 140, 168, 179, 194, 206, 218, 244. The data stored in Plaintiffs' and Class members' LastPass vaults included: login credentials and answers to security questions for hundreds of online accounts (including financial accounts, social media platforms, and other personal online accounts); login credentials for work email accounts and

servers; and copies of confidential documents containing sensitive health and financial information—including Social Security numbers, driver's license numbers, passport copies, credit card information, and cryptocurrency keys (collectively, "Private Information"). ¶¶ 14, 28, 42, 55, 70, 83, 96, 108, 121, 134, 149, 163, 175, 187, 201, 214, 224-230.

Plaintiffs reasonably relied on the explicit promises LastPass made via its website, privacy policy, advertising and marketing materials, and in other verbal and written statements. See, e.g., ¶¶ 237-241, 245, 262, 266 ("Safeguarding your data is what we do.").[2] Similarly, GoTo touts "industry-leading zero trust security." ¶ 4. But in or around August 2022, a threat actor achieved persistent entry (the "Data Breach") to Defendants' back-end developer environments and cloud-based servers.[3] ¶ 295. This began a four-month period of periodic reassurances, "investigations," and disingenuous displays of transparency, all which served to cover up the fact that Defendants did not appreciate the depth or implications of the intrusions into their systems, or what it would mean for their customers. ¶¶ 294, 298, 299, 302, 372. During that period, "the threat actor utilized their persistent access to impersonate [a LastPass employee]" which culminated in the threat actor obtaining a "cloud storage access key and dual storage container decryption keys[.]" ¶¶ 300-309. Using these keys, the threat actor "copied information from backup[,]" including unencrypted "customer account information and related metadata[.]" ¶¶ 309-310. Alarmingly, "[t]he threat actor was also able to copy a backup of customer vault data from the encrypted storage container[.]" ¶ 310. While LastPass maintains that master passwords were encrypted, it acknowledged "[t]he threat actor may attempt to use brute force to guess your master password and decrypt the copies of vault data they took." ¶ 311. Despite this

---

[2] Consistent with the explicit promises on its website, Section 4.2 of LastPass's Terms of Service for Personal Use states that LastPass "ha[s] implemented and maintain[s] appropriate organizational, administrative, and technical safeguards to protect your Content against any unauthorized access, loss, misuse, or disclosure." ¶ 262 (LastPass Terms of Service, https://www.lastpass.com/legal-center/terms-of-service/personal (last accessed October 11, 2023)).

[3] It remains unclear exactly when the Data Breach began, because Defendants have refused to provide this information. ¶ 295.

persistent intrusion, Defendants failed to provide any information to customers about security measures they should take beyond pointing to password best practices. ¶ 307. Finally, four months after the initial intrusion did Defendants offer *prospective* guidance to its customers, advising them to "consider minimizing risk by changing passwords of websites you have stored." ¶ 314.

LastPass published its fifth and most recent update on March 1, 2023, in which it explained that the threat actor infiltrated LastPass by stealing source code and technical data from the company in August 2022. LastPass admitted it had prematurely "declared this incident closed but later learned" information stolen in August 2022 was then leveraged to hack a LastPass employee. ¶ 316. For the first time, LastPass acknowledged the "data accessed [by the threat actor] from those backups included system configuration data, API secrets, third-party integration secrets, and *encrypted and unencrypted LastPass customer data*." ¶ 319 (emphasis in original). Among the customer data accessed, LastPass identified "customer metadata, and backups of all customer vault data." ¶ 320.

Defendants' official statements about the Data Breach have been misleading, false, and continue to omit important information. Despite their professed "commitment to transparency," Defendants failed to timely notify Plaintiffs and Class members or relevant authorities of the full nature of the Data Breach.[4] ¶¶ 9, 263. Instead of providing fulsome notice to those impacted by the Data Breach, Defendants repeatedly downplayed and minimized the incident to the detriment of Plaintiffs and the Class. ¶ 9. To date, neither Defendant has provided the most basic information about the Data Breach—such as when it began, how long the Data Breach persisted, or why LastPass was unable to detect it. ¶ 9. As a result, Plaintiffs and Class members still do not know what information was exposed or how long hackers have had it, leaving unclear what further steps—beyond those already recommended by the Defendants—they need to take to protect themselves. ¶ 9.

[4] Some Plaintiffs first learned about the Data Breach from friends (¶¶ 13, 120), employers (¶ 27), or online news reports (¶¶ 55, 82, 95, 148, 186, 213).

Plaintiffs and Class members, whose data was stolen and whose internet security has been permanently compromised, have already experienced significant and real harm as a result of the Data Breach, from actual theft to identity theft, malicious attacks on accounts, and fraud. ¶¶ 7, 16, 30, 123, 136, 151, 152, 189, 224-230. In addition to paying for a service that was not provided as advertised (¶¶ 48, 63, 76, 113, 127, 141, 168, 180, 194, 207, 219), some Plaintiffs incurred direct losses as a result of the Data Breach (¶¶224-230) and have and will continue to spend thousands of dollars (¶¶ 19, 46, 60, 87, 155, 178, 192, 205) and countless hours (¶¶ 17, 18, 31-2, 44, 58-9, 72-3, 85-6, 98-9, 110-1, 123-24, 137-38, 153-54, 165-66, 176, 190-91, 203-4, 216-17) responding to the Data Breach.

LastPass continues to assert that customer master passwords were not exposed in the Data Breach, but this is belied by Plaintiffs' own experiences. ¶ 355 ("Plaintiffs have lost cryptocurrency from accounts that could only be accessed using keys kept in their LastPass vaults."). LastPass claims "it would be extremely difficult to attempt to brute force guess master passwords for those customers who follow our password best practices." ¶ 358. But Plaintiffs disagree; Defendants leave out that they have not updated their customer password encryption requirements since 2018. ¶ 361.[5]

Defendants are in the security business and are therefore uniquely aware of the risks of cyberattacks and data breaches. ¶ 372. As a company in the business of storing and managing login credentials, identities, and passwords—literally the "keys to the kingdom"—for more than 33 million users and 100,000 businesses worldwide, LastPass knew it was among the most attractive targets for cybercriminals. ¶¶ 1, 242. In fact, prior to its acquisition by GoTo, LastPass experienced an extensive history of cybersecurity incidents. ¶¶ 281, 283-291. GoTo was aware that it too was an attractive target

[5] "Since 2018, [LastPass] [has] required a twelve-character minimum for master passwords[]" and "implementation of 100,100 phases of the Password-Based Key Derivation Function (PBKDF2), a password-strengthening algorithm that makes it difficult to guess your master password." ¶ 361. These requirements did not retroactively apply to existing accounts, and as LastPass acknowledges, a "master password [that] does not make use of the defaults above, [] would significantly reduce the number of attempts needed to guess it correctly." This has made especially vulnerable the vaults of customers whose LastPass master passwords predate the 2018 security update.

for cybercriminals, having been the target of one or more data breaches itself. ¶ 243. Despite Defendants' awareness of the risk, LastPass failed at its only job—protecting users' most sensitive and personal information. ¶1.

LEGAL STANDARD

When reviewing a pre-discovery motion to dismiss under either Federal Rule of Civil Procedure 12(b)(1) or 12(b)(6), a court must accept as true all well-pleaded facts and indulge all reasonable inferences in the plaintiffs' favor. *Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 371 (1st Cir. 2023). Plaintiffs are not required to allege every single fact that supports their claim in their complaint, but rather, must provide fair notice to the defendants and state a facially plausible legal claim. *Ocasio-Hernandez v. Fortuno-Burset*, 640 F.3d 1, 13 (1st Cir. 2011). Instead, the Court should draw on its judicial experience and common sense and may not disregard properly pled factual allegations even if actual proof of those facts seems improbable. *Id.*

ARGUMENT

A. Plaintiffs readily satisfy Article III standing and, if not, the appropriate action is to remand the actions Defendants removed.

Plaintiffs' claims readily satisfy Article III standing because they have suffered concrete, particularized injuries in fact that are fairly traceable to Defendants' Data Breach. Further, Defendants have already admitted that Plaintiffs satisfy Article III standing via their removal of some underlying actions to federal court, making dismissal inappropriate.

1. Plaintiffs have suffered concrete and particularized injuries-in-fact.

Plaintiffs allege actual, concrete, and particularized injuries-in-fact in their Consolidated Complaint as well as facts that establish a substantial risk of future identity theft, as Plaintiffs' personal information is now in the hands of cybercriminals who have already exploited this data to cause injury. While either of these two categories of injuries is sufficient to satisfy the standing requirements at the pleadings stage in the First Circuit, the Complaint properly pleads other categories of injury as well.

Webb, 72 F.4th at 373.

Plaintiffs' personal information has already been misused. Numerous Plaintiffs have alleged the theft of cryptocurrency from accounts only accessible using information stored in Plaintiffs' LastPass vaults (¶¶ 224-30) as well as unauthorized credit card charges and attempts (whether successful or unsuccessful) to open credit accounts (¶¶ 16, 19, 123, 151, 189, 229) stemming from the Data Breach.[6] These injuries alone are sufficient to establish standing. In *Webb*, the First Circuit concluded that "plausible allegations of actual misuse [of PII] . . . state a concrete injury under Article III." *Webb*, 72 F.4th 365, 373 (1st Cir. 2023) (citing *In re Equifax Inc. Customer Data Sec. Breach Litig.*, 999 F.3d 1247, 1262 (11th Cir. 2021); *see also Attias v. CareFirst, Inc.*, 865 F.3d 620, 627 (D.C. Cir. 2017); *In re Marriott, Int'l, Inc. Customer Data Sec. Breach Litig.,* 440 F. Supp. 3d 447, 459 (D. Md. 2020) ("*Marriott*") (standing satisfied with unauthorized charges and unauthorized accounts for lines of credit).

Similarly, Plaintiffs have alleged numerous instances where criminals have already committed identity theft, fraud, or engaged in scams using the Private Information that was compromised as a part of the Data Breach (¶¶ 16, 151, 189), as well as increased spam and phishing attacks (¶¶ 30, 123, 136). No fewer than nine of the sixteen named Plaintiffs have alleged that unauthorized parties have misused their data—either stealing or attempting to steal from them. ¶¶ 16, 30, 136, 151, 189, 223-230. This misuse is an invasion of a "an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical." *Beck v. McDonald,* 848 F.3d 262, 274 (4th Cir. 2017) (cleaned up); *see also Remijas v. Neiman Marcus Grp., LLC,* 794 F.3d 688, 690 (7th Cir. 2015) (standing satisfied when at least one named plaintiff alleged misuse or access of personal information); *Portier v. NEO Tech. Sols.*, 2019 WL 7946103, at *4 (D. Mass. Dec. 31, 2019),

[6] Plaintiffs have alleged that they stored access credentials to their other compromised accounts as well as PII in their LastPass vaults. *Id.* ¶¶ 14, 43, 70, 96, 122, 149, 175, 188, 224, 225, 227, 229, 230.

report and recommendation adopted, 2020 WL 877035 (D. Mass. Jan. 30, 2020); *Hutton v. Nat'l Bd. of Examiners in Optometry, Inc.*, 892 F.3d 613, 622-623 (4th Cir. 2018) ("[T]he Supreme Court long ago made clear that '[i]n interpreting injury in fact . . . standing [is] not confined to those who [can] show economic harm.'" (quoting *United States v. Students Challenging Regulatory Agency Procedures*, 412 U.S. 669, 686 (1973)). Thus, Plaintiffs' allegations of actual incidents of identity theft and fraud satisfy the injury-in-fact requirement.

Plaintiffs face additional substantial risk of immediate harm. In determining standing for claims for future risk of identity theft, the Court examines three "non-exhaustive" factors: (1) whether the plaintiffs' data has been exposed as the result of a targeted attempt to obtain that data; (2) whether any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud; and (3) whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud. *Webb*, 72 F.4th at 375 (citing *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 302 (2d Cir. 2021) and *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 153-54, 157 (3d Cir. 2022). Plaintiffs have pleaded each of these factors.

As discussed above, Plaintiffs have adequately pleaded that their own data was exposed and that their own data has been misused. *See supra,* 8-9. Plaintiffs have also alleged that they, at the invitation of LastPass, stored some of their most sensitive, important information in their LastPass vaults and through LastPass's services, as well as the login credentials for the most vital and important accounts that consumers hold. ¶¶ 14-16, 28-29, 42, 56, 70, 83, 96, 108, 121, 134, 149, 163, 188, 201, 214.[7] Thus, the information implicated in this data breach, by definition, satisfies the third factor identified by the *Webb* court. Plaintiffs in this action who have not yet experienced actual misuse have

[7] Plaintiffs stored personally identifying information in their LastPass vaults, including login credentials and passwords for (1) financial accounts; (2) email and social media accounts; (3) business and corporate accounts; and (4) cryptocurrency wallets and management accounts; as well as private documents and information contained within the LastPass notes and vaults including names, dates of birth, addresses, copies of birth certificates and driver's licenses social security numbers, and other personally identifying information.

nonetheless alleged the "risk of harm [that is] sufficiently imminent and substantial" to show Article III standing at the pleadings stage. *TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2210 (2021); *see also Hutton,* 892 F.3d at 622 (applications for credit cards had been made using the plaintiffs' stolen information sufficient to plead a concrete injury-in-fact, even though the plaintiffs "[did] not allege that they suffered fraudulent charges on their unsolicited [] credit cards[.]")).

Plaintiffs spent time and money dealing with the breach. Because Plaintiffs face an actual and imminent risk of concrete and particularized harm, they took steps after the breach to ensure that their information was protected and to prevent the Data Breach from causing them more harm.[8] *Defendants even recommended they take steps to mitigate this risk.* ¶ 314. As *Webb* holds, "time spent responding to a data breach can constitute a concrete injury sufficient to confer standing, at least when that time would otherwise have been put to profitable use." *Webb*, 72 F.4th 377 (citing *Hutton,* 892 F.3d at 622); see also *Marriott.*, 440 F. Supp. 3d at 460 ("[T]he injuries alleged by the Plaintiffs are not speculative, the costs of mitigating measures to safeguard against future identity theft support the other allegations and together readily show sufficient injury-in-fact to satisfy the first element of the standing to sue analysis."). Costs spent mitigating harm, especially when Plaintiffs have already experienced identity theft, are also sufficient to satisfy Article III standing. *Anderson v. Hannaford Brothers Co.*, 659 F.3d 151-154 (1st Cir. 2011) (reversing district court because plaintiffs' alleged mitigation costs were incurred in response to a data breach and actual misuse of PII, and were thus "reasonable" and "constitute[d] a cognizable harm under Maine law.").

Defendants offer cursory argument that Plaintiffs mitigation damages are "manufactured." MTD, at 26. But this is not summary judgment and Plaintiffs plausibly pleaded that their mitigation efforts have been necessary to avoid additional harm.[9] *See Hutton*, 892 F.3d at 622 ("Because the

[8] ¶¶ 17-19, 31-32, 44-46, 58-60, 72-73, 85-87, 98-99, 110-111, 123-124, 136-138, 151-155, 165-166, 176-177, 189-192, 203-205, 216-217.

[9] *See* n. 8, *supra*.

injuries alleged by the Plaintiffs are not speculative, the costs of mitigating measures to safeguard against future identity theft support the other allegations and together readily show sufficient injury-in-fact to satisfy the first element of the standing to sue analysis."); *Marriott*, 440 F. Supp. 3d at 460 ("[B]ecause the alleged actual and threatened harm to the Bellwether Plaintiffs is sufficiently non-speculative to establish injury-in-fact, the Bellwether Plaintiffs have also established injury-in-fact based on the alleged time and money spent to mitigate that harm."). As the *Marriott* court put it, "the two theories of injury-in-fact stand or fall together." *Id.* Here, they stand.

Plaintiffs did not get the benefit of their bargain. Plaintiffs also satisfy standing because they did not receive the online security that they bargained for. ¶¶ 48, 63, 76, 113, 127, 141, 168, 180, 194, 207, 219. This satisfies the standing requirement. *See Uzuegbunam v. Preczewski*, 141 S. Ct. 792, 800 (2021) ("[A] party whose rights are invaded can always recover . . . without furnishing any evidence of actual damage.") (citation omitted); *Hartigan v. Macy's, Inc.*, 501 F. Supp. 3d 1, 6 (D. Mass. 2020) ("The breach of a contractual right can constitute an injury sufficient to create standing."); *Marriott,* 440 F. Supp. 3d at 463 (finding that "Plaintiffs have adequately alleged injury-in-fact based on failure to receive the benefit of their bargain regarding data security."); *Salas v. Acuity-CHS, LLC*, 2023 WL 2710180, at *10 (D. Del. Mar. 30, 2023) (finding that a breach of contract is sufficient to confer nominal damages, and nothing further is required); *Carlsen v. GameStop, Inc.*, 833 F.3d 903 (8th Cir. 2016) (holding that the plaintiff's allegations he did not receive the data protection set forth in defendant's policies suffices to support standing); *In re Yahoo! Inc. Customer Data Sec. Breach Litigation,* 313 F. Supp. 3d 1113, 1130 (N.D. Cal. 2018) (finding that plaintiff adequately alleged benefit-of-the-bargain losses.). Plaintiffs allege that Defendants promised, through both express contract terms (¶¶ 295-330, 432-436) and implied promises (¶¶ 448, 451), that the credentials and PII kept in their LastPass accounts and in their vaults would be secure—indeed, the protection of the Plaintiffs' PII and other confidential information is not ancillary to the contracts in question—*it is the very focus* of the

contracts. ¶¶ 260-264. This more than satisfies Article III standing.[10]

To be clear, Plaintiffs are not claiming that they did not receive vaults to store account credentials and confidential information (including PII). Plaintiffs allege that Defendants explicitly marketed and promoted these vaults as "secure," and that these vaults were much less secure than advertised because of Defendants' failure to provide that promised security, such that the value of what they obtained in the contract was diminished in value from what they reasonably expected. ¶¶ 34, 48, 63, 76, 113, 127, 141, 168, 190, 194, 207, 219, 493. Plaintiffs' allegations clearly show a concrete injury in fact (loss of the benefit of the bargain), that Defendants were the cause of this injury (by failing to provide adequately secure storage), and redressability (compensation for the difference in value between what Plaintiffs would have exchanged, and what they did exchange).[11] These allegations are sufficient to satisfy Article III.

2. Plaintiffs' injuries are fairly traceable to the breach.

Defendants contend that Plaintiffs' injuries are not fairly traceable to the Data Breach because the Plaintiffs have "simply assumed a data breach compromised her nonpublic personal data." MTD, at 22. To support this, Defendants make the brazen claim that "[e]ncrypted vault data . . . like account usernames and passwords, access keys, and any other sensitive information a user chose to store as a secure note, remains encrypted and unreadable. And the only way to access and read encrypted vault data is with a user's master password, which Defendants never had or knew." *Id.* This is not a pleading defect, but a factual dispute, and is belied by Defendants' own statements to the contrary. ¶¶ 350,

[10] In other data breach cases where contract claims did not survive, the protection of that information was *ancillary* to the parties' agreement. *See Marriott,* 440 F. Supp. 3d at 463 (primary focus of contract was for hotel room); *Carlsen*, 833 F.3d 903 (8th Cir. 2016) (handling of personal information related to access paid subscription benefits); *In re Yahoo!*, 313 F. Supp. 3d at 1130 (focus of contract was purchase of a "premium email service").

[11] Defendants do not appear to challenge the redressability of Plaintiffs' injuries, and therefore Plaintiffs do not address this here.

354.[12] Regardless, it is not an issue that can be resolved on a Motion to Dismiss.

Article III does not require that Plaintiffs rule out all other possible causes of their injuries: Plaintiffs need only allege "that [defendants'] actions led to the exposure and actual or potential misuse of the plaintiffs' PII, making their injuries *fairly* traceable to [defendants'] conduct." *Webb*, 72 F.4th at 377 (citing *In re Evenflo Co., Inc., Mktg., Sales Pracs. & Prod. Liab. Litig.*, 54 F.4th 28, 41 (1st Cir. 2022), *cert. denied sub nom. Evenflo Co., Inc. v. Xavier, Mike, et al.*, 2023 WL 6377930 (U.S. Oct. 2, 2023) (emphasis added)); *see also Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 572 U.S. 118, 134 n.6 (2014) ("Proximate causation is not a requirement of Article III standing, which requires only that the plaintiff's injury be fairly traceable to the defendant's conduct."). Plaintiffs need only show "an obvious temporal connection between the [PII misuse] and the timing of the data breach" and that their allegations of misuse were "made in the context of allegations relating to harms [Plaintiffs] suffered because of the data breach." *Webb*, 72 F.4th at 374.

Plaintiffs here meet that standard. "[T]hey have lost access to accounts that were only accessible through their password vaults, and lost funds from cryptocurrency accounts that could only be accessed using keys saved in their vaults." *See, e.g.,* ¶¶ 8, 225, 230. And the information used to access those vaults could *only* be obtained through LastPass. ¶¶ 295-297. Further, these losses occurred immediately after the Data Breach—after August 2022. ¶¶ 16, 29, 136, 151, 223-30, 278. As Plaintiffs allege, the way in which hackers were able to access information that was only present in Plaintiffs'

[12] Defendants cite to several out-of-circuit cases that are factually distinguishable in support of their argument that Plaintiffs have failed to show a link between the breach and their alleged injuries. *See* MTD, at 23. *Baysal v. Midvale Indemnity Co.* involved a situation where there was no explanation of how obtaining someone else's driver's license numbers could allow a hacker to fraudulently open an account of any kind. 78 F.4th 976, 977 (7th Cir. 2023), *reh'g denied*, 2023 WL 6144390 (7th Cir. Sept. 20, 2023). *Peters v. St. Joseph Servs. Corp.* involved the dismissal for lack of standing of only the plaintiff's claim brought under the Federal Credit Reporting Act's private right of action (which Plaintiffs here have not alleged) and only because the plaintiffs failed to describe how the defendant's violation of the statute had proximately caused the injuries claimed. 74 F. Supp. 3d 847, 851 (S.D. Tex. 2015). *Peters*, 74 F. Supp. 3d at 851. And in *Springmeyer et al. v. Marriott International, Inc.* the court there compared the "conclusory" allegations in that case to the detailed, supported allegations in the complaint in a companion case. *See Marriott*, 440 F. Supp. at 454. Notably, co-lead counsel for the Plaintiffs in the instant action is also one of the co-lead counsel representing plaintiffs in the pending *Marriott* MDL.

vaults, and the only way in which hackers were able to get account information which Plaintiffs stored in their LastPass accounts, was through the Data Breach. Such injuries are directly traceable.

3. Defendants already conceded federal subject matter jurisdiction.

Finally, it is surprising that Defendants are challenging Plaintiffs' standing to bring this action, as they have already conceded Article III subject matter jurisdiction. *See* Notice of Removal, *Alan Murphy Jr. v. LastPass US, LP*, No. 23-cv-00627, ECF No. 1 (Feb. 1, 2023) ("*Murphy* Action"); Notice of Removal of Civil Action from State Court, *John Doe v. LastPass US, LLC*, No. 23-cv-01723-VC, ECF No. 1 (Apr. 10, 2023) ("*Doe* Action").

The Defendants requested that the *Murphy* and *Doe* Actions (which were ultimately consolidated here) be removed because federal—not state—courts have subject matter jurisdiction over Plaintiffs' claims. *See Murphy* Action, ECF No. 1 at 4 ("[T]he Court has original subject matter jurisdiction"), *Doe* Action, ECF No. 1 at 2 (requesting removal "on the grounds that this Court has jurisdiction over this civil action pursuant to 28 U.S.C. §§ 1332, 1441, and 1446, and all other applicable bases for removal."). "The part[ies] invoking federal jurisdiction"—here, the Defendants—"bear[] the burden" of establishing standing under Article III. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992).

Defendants seek to game the system by removing based on Article III jurisdiction and then seeking dismissal for failure to satisfy that very same standard. As courts have held, it is inappropriate for "a defendant [to] tr[y] to have it both ways by asserting, then immediately disavowing, federal jurisdiction, apparently in hopes of achieving outright dismissal, with prejudice, rather than the remand required by § 1447(c)." *Mocek v. Allsaints USA Ltd.*, 220 F. Supp. 3d 910, 914 (N.D. Ill. 2016) (granting plaintiff's motion for attorneys' fees after defendant removed and then sought dismissal); *see also Martin v. Franklin Cap. Corp.*, 546 U.S. 132, 141 (2005) (same); *Barnes v. ARYZTA, LLC*, 288 F. Supp. 3d 834,

840 (N.D. Ill. 2017) (same).[13]

If the Court contemplates granting Defendants' motion, and agrees that they had no reasonable basis for removing the *Murphy* and *Doe* Actions, remanding those cases (not dismissal) and granting Plaintiffs' costs and attorneys' fees would be the appropriate remedy for managing those claims. *See Mocek*, 220 F. Supp. 3d at 914-15; *Pitre v. Wal-Mart Stores, Inc.*, 2019 WL 5294397, at *9 (C.D. Cal. Oct. 18, 2019) ("[R]emand—consistent with [28 U.S.C. § 1447(c)]'s use of *shall*—is generally mandatory.") (emphasis in original). Defendants cannot have it both ways.

B. Plaintiffs state viable contract-based claims under 12(b)(6).

Plaintiffs allege detailed factual allegations in the Complaint, such that their claims are not only plausible, but well-supported. Defendants violated Plaintiffs' common law and statutory rights, and the Complaint puts Defendants on notice with sufficient detail to satisfy the liberal Federal pleadings standard. Defendants motion under Federal Rule of Civil Procedure 12(b)(6) should be denied.

1. Defendants' actions have violated contracts with consumers.

Plaintiffs have alleged with specificity which of the Terms of Service were breached, which of Defendants' acts and omissions constituted breaches, and damages arising therefrom—more than enough to state a claim for breach of express contract. *See Sourcing Unlimited, Inc. v. Elektroteks, LLC*, 2021 WL 2875713, at *13 (D. Mass. July 8, 2021) ("Although the general rule is that plaintiffs must point to specific contractual obligations that were allegedly breached, . . . the First Circuit has encouraged courts to allow breach of contract claims to survive motions to dismiss if the contract could plausibly be read in the plaintiff's favor and the complaint's allegations suggest a breach.") (*citing Young v. Wells Fargo Bank, N.A.*, 717 F.3d 224, 233 (1st Cir. 2013) (citation omitted)).

In particular, Plaintiffs have detailed Defendants' failures to "implement[] and maintain

[13] Plaintiffs have not submitted a costs and fees request because they believe that they have satisfied Article III standing. However, if the Court were to grant Defendants' motion to dismiss for lack of Article III standing, Plaintiffs request the opportunity to submit a request for fees and expenses.

appropriate organizational, administrative, and technical safeguards" as promised in the Terms of Service. ¶¶ 432-436. For example, "LastPass failed to adopt and comply with industry standard regulations" in that LastPass "only require[d] 100,100 iterations of the PBKDF2 algorithm to secure customers' master passwords, which is well below the standard 310,000 iterations recommendation by the Open Web Application Security Project." *Id.*, ¶¶ 273, 436. The CAC further alleges that "at the time of the Data Breach, LastPass had failed to update its master password encryption requirements since as early as 2018, a lifetime by cybersecurity standards." *Id.* at ¶ 274. The CAC also details the failures in LastPass's master password structure, *id.* at ¶ 276, and that there was no system to ensure copies of customer vaults were not made, *id.* at ¶ 277.

LastPass also failed to "implement and maintain adequate safeguards and procedures to prevent the unauthorized access to Plaintiffs' and Class Members' PII."[14] *Id.*, ¶ 436. The security measures in place at the time of the August 2022 intrusion were not appropriate; this is evidenced by the nature and scope of the Data Breach, and the Plaintiffs identify numerous steps Defendants *eventually* took but they should have taken in the first place. *Id.* at ¶¶ 312-13, 317. This is an indication that the "security measures" were insufficient.

Additionally, the Complaint alleges that LastPass' organizational and administrative safeguards were deficient. Defendants acknowledge that LastPass's terms of service contemplate that LastPass will "provid[e] notice and tak[e] actions designed to promptly resolve any security issues . . . ," (MTD, at 35),[15] but LastPass failed to competently investigate and assess the danger posed to its users, and

[14] Namely, LastPass (i) did not require that customers who started accounts prior to 2018 "update their shorter, less-secure master passwords to a twelve-character minimum," *id.* at ¶ 276; (ii) "did not manage its own cybersecurity systems to ensure that copies were not made of customer password vaults," *id.* at ¶ 277; (iii) permitted its employee to deploy third-party software in a manner that created the vector for the actors to gain access to LastPass' systems, *id.* at ¶ 318; and allowed the intruder to access LastPass' systems for weeks or months, *id.* at ¶ 318.

[15] Defendants argue that the Terms of Service do not promise "100% cybersecurity" and point to provisions in the Terms of Service contemplating data security incidents occurring. "[T]hese disclaimers do not absolve Defendants of any contractual obligation to take reasonable steps to protect users' PII." See *In re Yahoo!*

repeatedly issued false assurances to its users without acknowledging the extent of the Data Breach. ¶¶ 295-30, 309-14. Moreover, despite claiming on August 25, 2022 that they "implemented enhanced security measures," on November 30, Defendants admitted that the "unauthorized party, using information obtained in the August 2022 incident, was able to gain access to certain elements of our customers' information." ¶¶ 262, 304; 306. Ultimately, this failure exacerbated the "unauthorized access, loss, misuse, or disclosure" of Plaintiffs' PII, as Defendants prevented their users from understanding the risks posed and protecting themselves. ¶ 366.

Defendant's reliance on *Kuhns v. Scottrade, Inc.*, is misplaced, as plaintiffs in that case failed to allege any details supporting their breach of contract claim, instead providing "just bare assertions that [defendant's] efforts failed to protect customer PII." 868 F.3d 711, 717 (8th Cir. 2017). Here, Plaintiffs have pleaded facts sufficient to conclude there is "substantial certainty" that Defendants breached their contractual obligations.[16]

Defendants' second line of defense fails as well, because the limitation of liability provisions in the Terms of Service are unconscionable[17] and, in any case, do not preclude liability for direct

Inc. Customer Data Sec. Breach Litig., 2017 WL 3727318, at *45 (N.D. Cal. Aug. 30, 2017) (holding that plaintiffs had alleged that defendants violated promise in the terms of service to "limit access to personal information" about Plaintiffs").

16 *See Marriott,* 440 F. Supp. at 484-85 (denying a motion to dismiss an express contract claim based on privacy statements providing that defendants would use "reasonable organizational, technical and administrative measures to protect [its customers'] Personal Data" and would "safeguard your information using appropriate administrative, procedural and technical safeguards," explaining "[w]hile the parties may dispute the contours of these duties and whether they were breached after discovery, at this stage Plaintiffs have plausibly alleged the terms of the contract regarding data security").

17 To the extent required, Plaintiffs respectfully seek leave to amend to articulate the basis of their claims more fully for unconscionability. *See Yahoo*, 2017 WL 3727318 at *45 ("The Court grants leave to amend because Plaintiffs may be able to allege that the limitations in Defendants' Terms of Service are unconscionable."); *Yahoo*, 313 F. Supp. 3d at 1138 (holding that "Plaintiffs have adequately pled the necessary elements of procedural and substantive unconscionability" regarding defendants' limitation of liability clause). Under Massachusetts law, "'[t]o prove that the terms of a contract are unconscionable, a plaintiff must show both substantive unconscionability (that the terms are oppressive to one party) and procedural unconscionability (that the circumstances surrounding the formation of the contract show that the aggrieved party had no meaningful choice and was subject to unfair surprise).'" *Machado v. System4 LLC*, 471 Mass. 204, 218, 28 N.E.3d 401, 414 (2015) (quoting *Storie vs. Household Int'l, Inc.*, U.S. Dist. Ct., No. 03-40268, 2005 U.S. Dist. LEXIS 40292 (D. Mass. Sept. 22, 2005)). Without the benefit of discovery, Plaintiffs have not yet had the opportunity to make these showings.

damages suffered by Plaintiffs. *See In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 WL 3727318, at *45 (N.D. Cal. Aug. 30, 2017) (holding contractual clause precluding liability for "punitive, indirect, incidental, special, consequential or exemplary damages" did not "limit Defendants' liability for direct damages"). Direct damages are damages that "flow according to common understanding as the natural and probable consequences of the breach, that is, those arising naturally according to the usual course of things, from such breach of contract itself." *Boylston Housing Corp. v. O'Toole*, 321 Mass. 538, 562, 74 N.E.2d 288 (1947) (internal quotations omitted). Here, all of Plaintiffs' damages "arise naturally" from Defendants' breach because Plaintiffs contracted with Defendants to protect their PII, and Defendants failed to provide the service that would do so. Accordingly, Plaintiffs have adequately pleaded their claims for breach of express contract.

2. Plaintiffs' implied contract claims have merit.

Plaintiffs have alleged with specificity, in the alternative, that an implied contract with Defendants existed and that contract was breached.[18] "An implied-in-fact contract arises from conduct that would lead a reasonable person in the other party's position to infer a promise in return for performance or promise. . . ." *Prescott v. Morton Int'l, Inc.*, 769 F. Supp. 404, 410 (D. Mass. 1990) (quotations omitted). Here, Plaintiffs have alleged the existence of an implied contract by which they "provided and entrusted their PII and financial information to Defendants" and Defendants "agreed to safeguard and protect [Plaintiffs' PII], to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and compromised or stolen."[19] ¶¶ 448, 451. Courts have recognized this as a valid basis for an implied contract. *See Shedd v. Sturdy Mem'l Hosp., Inc.,* 2022 WL 1102524, at *10 (Mass. Super. Apr. 5, 2022)

[18] Plaintiffs bring this claim "in the alternative to the breach of contract claim on behalf of individuals and entities which paid for LastPass accounts, and in the first instance on behalf of individuals and entities which did not pay for LastPass accounts." ¶ 442.

[19] Plaintiffs have alleged all required aspects of a contract implied by a course of conduct, including a meeting of the minds on specific terms. ¶¶ 444-49.

(finding "dismissal is not appropriate" for an implied contract claim because "[w]hen a patient hands over sensitive information to receive medical care, they expect an implicit assurance that the information will be protected").[20] Plaintiffs have alleged that Defendants breached this contract for the reasons discussed above. *See supra* B.1.

The terms of service do not preclude this implied contract because they supplement rather than contradict the provisions thereof. *See Prescott v. Morton Int'l, Inc.*, 769 F. Supp. 404, 410 (D. Mass. 1990) (denying summary judgement of implied contract claim because "[a] separate implied-in-fact contract governing the dissemination of information between the parties would not be contradictory" to the parties' express contract, which "does not memorialize their entire relationship"). Defendants argue that the mere existence of an express contract between the parties precludes the possibility of an implied contract. MTD at 36. This is incorrect. Only "an existing express contract covering the same subject matter" can preclude an implied contract. *Omori v. Brandeis Univ.*, 635 F. Supp. 3d 47, 53 (D. Mass. 2022) (holding that the existence of two express contracts did not preclude an implied contract because "[a]lthough [the express contracts] contain express terms regarding certain matters related to tuition and fees, neither is dispositive as to whether [defendant] had an obligation to refund plaintiffs upon ceasing to provide an in-person education to them"); *cf. CSX Transp., Inc. v. Mass. Bay Transp. Auth.*, 697 F. Supp. 2d 213, 224 (D. Mass. 2010) (declining to imply an indemnification provision because the parties' agreement "expressly governs any indemnification agreement that may exist").

[20] *See also Castillo v. Seagate Tech., LLC,* 2016 WL 2980242, at *9 (N.D. Cal. Sept. 14, 2016) ("While [Defendant] made no explicit promises as to the ongoing protection of personal information, it is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of Social Security Numbers or other sensitive personal information would not imply the recipient's assent to protect the information sufficiently."); *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1176 (D. Minn. 2014) (holding that the plaintiffs had sufficiently pleaded "an implied contract in which Plaintiffs agreed to use their credit or debit cards to purchase goods at Target and Target agreed to safeguard Plaintiffs' personal and financial information").

3. Defendants have violated their covenants of good faith and fair dealing.

"In determining whether a party violated the implied covenant of good faith and fair dealing, we look to the party's manner of performance." *Robert & Ardis James Found. v. Meyers*, 474 Mass. 181, 189, 48 N.E.3d 442, 450 (2016). Defendants assert that Plaintiffs' claim fails because they have not pleaded the "*destruction* of rights," (MTD, at 38), but Plaintiffs have alleged a breach based on Defendants' unfair dealing,[21] which prevented them from obtaining the bargained-for benefits of the contract. *See Sykes v. RBS Citizens, N.A.*, 2 F. Supp. 3d 128, 139 (D.N.H. 2014) (determining that a plaintiff had sufficiently alleged a destruction of his contractual rights based on the defendant's failures to provide notice, fix billing errors, and timely respond to his requests for information). Defendants' reliance on *Bourgeois v. Blue Cross Blue Shield of Mass.*, 531 F. Supp. 3d 407, 416 (D. Mass. 2021) is wholly inapposite. The court in *Bourgeois* found no breach of the covenant because it found no contract at all and, moreover, plaintiffs had failed to state any facts suggesting that defendant "acted in a manner to destroy or injure their rights." *Id.*.

C. Plaintiffs' negligence and negligence *per se* claims must stand.

Plaintiffs have adequately plead the elements of negligence and negligent misrepresentation under Massachusetts law, and the economic loss doctrine does not bar their recovery in tort, because Defendants had independent duties to the Plaintiffs. Defendants motion to dismiss Plaintiffs' negligence-based claims should be denied.

1. Plaintiffs adequately plead claims for negligence and negligent misrepresentation.

Defendants do not contest that Plaintiffs met their pleading burden both with respect to the

[21] Defendants breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PII and financial information, failing to timely and accurately disclose the Data Breach to Plaintiffs and Class Members and continued acceptance of PII and financial information and storage of other personal information after Defendants knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach. ¶ 485.

existence of Defendants' duty and Defendants' breach of that duty.[22] ¶¶ 295-324. *See Webb v. Injured Workers Pharmacy, LLC*, 2023 WL 5938606, at *2 (D. Mass. Sept. 12, 2023). And, as discussed previously, Plaintiffs have sufficiently pleaded cognizable injury. ¶¶ 11-230, 278, 400-404.

The remaining element of negligence, "causation[,] is a fact-intensive question that the court cannot resolve at the pleading stage of the litigation." *Webb*, 2023 WL 5938606, at *2. (citing *Jupin*, 447 Mass. at 146 ("[W]hether the defendant's breach and the damage were causally related" is in "the special province of the jury.")). Defendants argue that Plaintiffs failed to plead proximate cause because Plaintiffs' data was encrypted when stolen and "could only be accessed using Plaintiffs' master passwords, which they created and only they knew and Defendants never had." MTD, at 30. But this is disputed, and Defendants have previously admitted that a threat actor might access the vault data using "brute force." ¶¶ 311, 354. Plaintiffs thus sufficiently "plead facts that plausibly connect the alleged breach of duty to the harm plaintiffs suffered." *Portier*, 2019 WL 7946103, at *14 (citation omitted).

Moreover, previous security vulnerabilities, including previous data breaches (¶¶ 243, 284-291), "should have sufficed to put [Defendants] on notice of the risks and consequences of its failure to adequately safeguard sensitive customer PII." *Webb*, 2023 WL 5938606, at *2. Plaintiffs' damages flow as a direct and foreseeable result of Defendants' failure to implement proper security measures. ¶ 416. *See Reid v. City of Boston*, 95 Mass. App. Ct. 591, 601 (2019) ("It is irrelevant whether [the defendant] foresaw or should have foreseen the *specific* danger that occurred.... It is sufficient that the same general kind of harm was a foreseeable consequence of the defendant's risk-creating conduct." (quoting *Jupin*, 447 Mass. at 149 n.8) (alteration in original)). Plaintiffs' Complaint sufficiently alleges

[22] Under Massachusetts law, "[t]o prevail on a negligence claim, a plaintiff must prove that the defendant owed the plaintiff a duty of reasonable care, that the defendant breached this duty, that damage resulted, and that there was a causal relation between the breach of the duty and the damage." *Jupin v. Kask*, 447 Mass. 141, 146 (2006).

that Defendants proximately caused Plaintiffs' injuries.

2. Defendants' economic loss arguments fail.

Defendants contend that Plaintiffs' negligence claim is barred by the economic loss doctrine, yet an identical argument was recently rejected twice by this court in two data breach cases, *Webb*, 2023 WL 5938606, at *3 and *Portier*, 2019 WL 7946103, at *22 (holding that Massachusetts is among those states "that permit recovery for economic losses in data breach cases").

Because Defendants' duty to protect consumers' PII is imposed by several state and federal laws[23] (¶ 514), independent and apart from any contract, the economic loss rule does not apply. *See Strategic Energy, LLC v. W. Mass. Elec. Co.*, 529 F. Supp. 2d 226, 236 (D. Mass. 2008) (negligent breach exception to economic loss doctrine applies where the breach is a violation of "an independent duty imposed by law that regulates the relationship between the parties" (citations and internal quotation marks omitted)); *see also Arthur D. Little Int'l, Inc. v. Dooyang Corp.*, 928 F. Supp. 1189, 1203 (D. Mass. 1996) (economic loss doctrine does not apply to claims for "negligent breach of contractual duties"); *Szulik v. State St. Bank & Trust Co.*, 935 F. Supp. 2d 240, 271 (D. Mass. 2013) ("Although the duty arises out of the contract and is measured by its terms, negligence in the manner of performing that duty as distinguished from mere failure to perform it, causing damage, is a tort." (quoting *Anderson v. Fox Hill Vill. Homeowners Corp.*, 424 Mass. 365, 368 (1997))). Plaintiffs' claims thus are not barred by the economic loss doctrine.

Defendants also fail to recognize Plaintiffs' injuries of anxiety, emotional distress, and loss of privacy as personal injury, another exception to the economic loss doctrine. ¶ 428. "'[P]ersonal injury' can be satisfied by a claim of emotional distress." *Webb*, 2023 WL 5938606, at *3 (citing *McCormick v. Lischynsky*, 2019 WL 3429242, at *5 (D. Mass. July 30, 2019)); *Maio v. TD Bank, N.A.*, 2023 WL

[23] For example, Plaintiffs have pleaded violations of duties imposed by the FTC Act, 15 U.S.C. § 45, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05.

2465799, at *4 (D. Mass. Mar. 10, 2023) (allegations including anxiety sufficient to overcome motion to dismiss negligence claim on economic loss doctrine grounds). As in *Webb*, this Court should reject Defendants' reliance on *In re TJX Cos. Retail Sec. Breach Litig.*, 564 F.3d 489 (1st Cir. 2009) and *Cumis Ins. Soc'y, Inc. v. BJ's Wholesale Club, Inc.*, 455 Mass. 458 (2009). 2023 WL 5938606, at *3. "[T]he legal landscape concerning liability for data breaches and identity theft is substantially different than it was when *TJX* and *Cumis* were decided [over] ten years ago." *Portier*, 2019 WL 7946103 at *18.

3. Plaintiffs' negligent misrepresentation claim is adequately pleaded and not barred by the merger clause in Defendants' Terms of Service.

Plaintiffs' allegations of negligent misrepresentation are clear cut and properly pled.[24] In the ordinary course of their business, Defendants served as a trusted steward of highly sensitive information by representing that they understood data security and took necessary steps to safeguard PII. ¶¶ 237, 245, 248-49, 257-66, 269-71. Plaintiffs relied on Defendants' representations that they would maintain the security and integrity of Plaintiffs' data. ¶¶ 20, 33, 47, 62, 75, 90, 101, 112, 126, 140, 168, 179, 194, 206, 218. LastPass represented that it secured Plaintiffs' PII, acknowledged it knew it was protecting information that "hackers love" (¶ 269; *see also* ¶¶ 243, 262, 270-71), and held itself out as an industry leader in online security (¶¶ 4, 237). Defendants should have ensured that these representations were current, accurate, and truthful so that Plaintiffs were "fully informed of the risks [] presented." *Corrigan v. Covidien LP*, 2022 WL 17094687, at *7 (D. Mass. Nov. 21, 2022). Defendants' failure to do so gives rise to a claim for negligent misrepresentation. *See id.* at *6-7 (upholding negligent misrepresentation claim); *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 371 F. Supp. 3d 1150, 1177 (N.D. Ga. 2019) (same).

[24] To assert a claim for negligent misrepresentation under Massachusetts law, a plaintiff must allege that a defendant: (1) in the course of its business, (2) supplied false information for the guidance of others, (3) in their business transactions, (4) causing and resulting in pecuniary loss to those others, (5) by their justifiable reliance on the information, and (6) that the defendant failed to exercise reasonable care or competence in obtaining or communicating the information. *AcBel Polytech, Inc. v. Fairchild Semiconductor Int'l, Inc.*, 928 F.3d 110, 122 (1st Cir. 2019); *Elec. Ins. Co. v. Great S. Fin. Corp.*, 2016 WL 1452338, at *6 (D. Mass. Apr. 13, 2016).

Defendants ignore Plaintiffs' allegations and instead claim Plaintiffs have not satisfied a heightened pleading standard.[25] However, Plaintiffs plead specific representations, on specific dates, in which Defendants: (i) held themselves out as industry leaders in the sale of online security (¶¶ 4, 237); and (ii) made specific representations that they would comply with federal law, industry data security protocols, and a compliance program that includes third-party audits and certifications to ensure that Plaintiffs' PII was secure. ¶¶ 271, 269-71, 432-35). By misreporting these security efforts, Defendants supplied false information used to guide Plaintiffs and others about the safety of their PII. *See In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 975 (S.D. Cal. 2014) (holding that defendants' "representations regarding reasonable security and industry-standard encryption" were "actionable misrepresentations" pled by Massachusetts plaintiff), *order clarified by* 2014 WL 12603117 (S.D. Cal. Feb. 10, 2014). Defendants knew of previous security vulnerabilities as well, having both been the target of more than one data breach. ¶¶ 243, 284-291. That independent entities also identified specific flaws in LastPass's security protocols, including bugs that allowed for the extraction of passwords and credentials, should have further warned Defendants of their deficient data security measures. ¶¶ 286-90. "The critical question is whether the [defendant] 'failed to exercise reasonable care or competence in obtaining or communicating the information.'" *DeWolfe v. Hingham Ctr., Ltd.*, 464 Mass. 795, 800 (2013) (quoting *Gossels v. Fleet Nat'l Bank*, 453 Mass. 366, 372 (2009)). By not reporting true and accurate representations concerning the safety and efficacy of their online products, Defendants failed to exercise reasonable care or competence in communicating this important information to users of their product. Instead, LastPass explicitly markets its password

[25] Federal courts analyzing the applicability of a heightened pleading standard to a negligent misrepresentation claim have concluded that "[Rule 9(b)] likely does not apply where the core allegation is negligence." *Gardner v. Simpson Fin. Ltd. P'ship*, C.A. 2012 WL 1109104, at *4 n.12 (D. Mass. Mar. 30, 2012) (citing *Mass. Sch. of Law at Andover, Inc. v. Am. Bar Ass'n*, 142 F.3d 26, 41 (1st Cir. 1998); *see also Grafton Partners, LLC v. Barry & Foley Motor Transp., Inc.*, 2007 WL 1418529, at *3 (Mass. Super. Ct. Apr. 9, 2007) ("Negligent misrepresentation is not a claim that must be pled with specificity."). Plaintiffs' allegations sound in negligence rather than fraud; however, as Plaintiffs abundantly demonstrate, Plaintiffs' allegations satisfy either Rule 8 or Rule 9(b).

management service as essential because "[d]ata breaches are on the rise[.]" ¶ 258.

As alleged, Defendants knew that Plaintiffs would rely on their representations, because no reasonable user would provide PII to LastPass if they did not believe that Defendants were maintaining the highest level of security reasonably attainable by "a pioneer in cloud security technology." ¶ 237. Building off its reputation and representations regarding data security, LastPass developed, offered, and sold "award-winning password and identity management solutions that are convenient, effortless, and easy to manage" to customers like Plaintiffs. *Id.* Thus, Defendants held themselves out as leaders in combatting cybersecurity threats and fostered Plaintiffs' reliance on its specialized knowledge. These representations resulted Plaintiffs and Class Members' losses. ¶ 416.

Lastly, Plaintiffs' reliance is not barred by the boilerplate merger clause in the parties' terms of service. "[W]here fraud and deceit are involved, general contractual disclaimers and exculpatory clauses have not automatically prevented a plaintiff from litigating his reasonable reliance on the misrepresentations in question." *Coughlin v. Gascombe*, 2000 Mass. App. Div. 321, 2000 WL 1880260, at *3 (Dist. Ct. 2000). There is no evidence that the merger clause "or any other exculpatory provision of the standard [terms of service] was ever discussed, much less negotiated and compromised, by the parties." *Id.* at *4; *compare Greenery Rehab. Grp., Inc. v. Antaramian*, 36 Mass. App. Ct. 73, 628 N.E.2d 1291, 1293 (1994) ("Representations and Warranties" and "Acceptance of the Deed" clauses in the parties' agreement were not "boilerplate" because they were specific compromises achieved after lengthy negotiations between the parties, barring misrepresentation claim). Regardless, many of Defendants' misrepresentations *are* contained in their terms of service. *See*, *e.g.*, ¶¶ 262, 432-35. Thus, Plaintiffs have adequately pleaded their negligent misrepresentation claim.

D. Defendants have violated their fiduciary duties to Plaintiffs.

Defendants' motion to dismiss the breach of fiduciary duty claim should be denied because Plaintiffs sufficiently allege a special relationship between Defendants and Plaintiffs and Class

Members. *See* ¶¶ 466-70. A wide range of circumstances can give rise to a fiduciary relationship. *Laker v. Freid*, 854 F. Supp. 923, 927-28 (D. Mass. 1994); *Korper v. Weinstein*, 57 Mass. App. Ct. 433, 437, (Mass. App. Ct. 2003) ("[T]he circumstances [that] may create a fiduciary relationship are so varied that it would be unwise to attempt the formulation of any comprehensive definition that could be uniformly applied in every case.") (citation omitted). "Whether or not a fiduciary relationship existed is a factual question to be decided by a jury." *Wilson Farm, Inc. v. Berkshire Life Ins. Co.,* 2002 WL 31440151, *8 (Mass. Super. 2002).

Massachusetts courts have recognized that even in business transactions a fiduciary "relationship can develop where one party reposes its confidence in another." *Katz v. Belveron Real Est. Partners, LLC*, 28 F.4th 300, 311–12 (1st Cir. 2022) (quoting *Indus. Gen. Corp. v. Sequoia Pac. Sys. Corp.*, 44 F.3d 40, 44 (1st Cir. 1995)) (citations omitted). To determine this, "courts look to the defendant's knowledge of the plaintiff's reliance and consider the relation of the parties, the plaintiff's business capacity contrasted with that of the defendant, and the readiness of the plaintiff to follow the defendant's guidance in complicated transactions wherein the defendant has specialized knowledge." *Katz*, 28 F.4th at 312 (quoting *Smith v. Jenkins*, 732 F.3d 51, 63 (1st Cir. 2013) (quoting *Indus. Gen. Corp.*, 44 F.3d at 44) (internal quotation marks omitted)).

Here, Defendants have held themselves out as having specialized knowledge regarding data security. ¶¶ 3, 4, 6. Due to Defendants' specialized knowledge, Plaintiffs and Class Members put their trust and confidence in Defendants' judgment, honesty, and integrity in protecting their PII and the various accounts that could be accessed through use (or misuse) of that PII. ¶ 467. Defendants knew that Plaintiffs and Class Members were relying on them, and Defendants accepted this trust and confidence when they accepted PII from Plaintiffs and Class Members. ¶ 468. Defendants became guardians of Plaintiffs' and Class Members' PII. ¶ 470. Plaintiffs have sufficiently put Defendants on notice of their claim, which is all they need do at the pleadings stage. *See Pearce v. Duchesneau Grp., Inc.*,

392 F.Supp.2d 63, 70–72 (D. Mass. 2005) ("On a motion to dismiss, the plaintiff is not obligated to prove that a fiduciary relationship existed. Rather, she need only put the defendants on notice of her claim.").

E. Plaintiffs are not precluded from seeking damages for unjust enrichment and declaratory relief.

Plaintiffs' unjust enrichment claim is plead in the alternative to their other claims.[26] ¶ 490. *Lass v. Bank of Am., N.A.*, 695 F.3d 129, 140 (1st Cir. 2012) (citing *Vieira v. First Am. Title Ins. Co.*, 668 F. Supp. 2d 282, 294-95 (D.Mass. 2009) (Rule 8(d) "permits Plaintiffs to plead alternative and even inconsistent legal theories, such as breach of contract and unjust enrichment, even if Plaintiffs only can recover under one of these theories")); *see also Webb*, 2023 WL 5938606, at *4 ("[A]t the pleading stage, a plaintiff is permitted to plead claims in law and equity in the alternative.") (citing *Chang v. Winklevoss*, 95 Mass. App. Ct. 202, 211 (Mass. App. Ct. 2019)); *Karter v. Pleasant View Gardens, Inc.*, 248 F. Supp. 3d 299, 311–12 (D. Mass. 2017) (denying motion to dismiss unjust enrichment claim).[27]

Defendants also ask the court to exercise its discretion to dismiss Plaintiffs' claim for declaratory relief because of the alleged availability of adequate legal remedies under state law. MTD, at 39. Plaintiffs' Eighth Claim seeks declaratory *and* injunctive relief. ¶¶ 499-507. Plaintiffs seek "prospective injunctive relief requiring LastPass to employ adequate security protocols consistent with law and industry standards to protect consumers' PII from future data breaches." ¶ 504. Plaintiffs have sufficiently alleged that the risk of another breach is real, immediate, and substantial. ¶ 505. As

[26] To prevail on a claim for unjust enrichment, Plaintiffs must establish that: (1) Defendants knowingly received a benefit (2) at Plaintiffs' expense (3) under circumstances that would make retention of that benefit unjust. *Karter v. Pleasant View Gardens, Inc.*, 248 F. Supp. 3d 299, 310–11 (D. Mass. 2017) (citing *Frappier v. Countrywide Home Loans, Inc.*, 645 F.3d 51, 58 (1st Cir. 2011)). "[A] claim for unjust enrichment does not require consideration, but there must be 'unjust enrichment of one party and unjust detriment to another party.'" *Karter*, 248 F. Supp. 3d at 311. Plaintiffs have sufficiently pled the elements of unjust enrichment. *See* ¶¶ 491-98.

[27] Defendants' reliance on *Fernandes v. Havkin*, 731 F. Supp. 2d 103, 114 (D. Mass. 2010), is misplaced—*Fernandes* was decided on summary judgment, not on a motion to dismiss. *See In re Auto. Parts Antitrust Litig.*, 29 F. Supp. 3d 982, 1020–21 (E.D. Mich. 2014) (denying motion to dismiss an unjust enrichment claim and stating that Fernandes does not dictate a contrary conclusion).

Defendants' ongoing wrongful conduct cannot be remedied by monetary damages, injunctive relief is appropriate. *See, e.g., Brooks v. Thomson Reuters Corp.*, 2021 WL 3621837, at *11 (N.D. Cal. Aug. 16, 2021) ("[T]he prospect of paying damages is sometimes insufficient to deter a defendant from engaging in an alleged unlawful, unfair, or fraudulent business practice"); *In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d 1130, 1141 (C.D. Cal. 2021) (injunctive claims upheld where a data breach was sufficiently likely to recur); *Leonard v. McMenamins, Inc.*, 2022 WL 4017674, at *6 (W.D. Wash. Sept. 2, 2022) (having alleged an imminent and substantial risk of harm resulting from a future breach, plaintiffs have standing to pursue injunctive relief).

The cases upon which Defendants rely are distinguishable. In *Wilton v. Seven Falls Co.*, 515 U.S. 277 (1995), the District Court stayed the case because the plaintiffs filed a state court suit regarding the same coverage issues raised in the federal action. Here, there is no parallel state court action. In *Rudolph v. Hudson's Bay Co.*, 2019 WL 2023713 (S.D.N.Y. May 7, 2019), the plaintiff did not seek injunctive relief. Finally, in *Fox v. Iowa Health Sys.*, 399 F. Supp. 3d 780 (W.D. Wis. 2019), the plaintiffs sought declaratory relief under the Wisconsin Deceptive Trade Practices Act ("WDTPA"), even though the court was already dismissing the plaintiffs' claims under the WDTPA (and related statutes in Illinois and Iowa). Here, the court has not dismissed any of Plaintiffs' other claims, and Plaintiffs are not seeking as part of their declaratory relief a declaration regarding one of their other claims.

F. Plaintiffs' consumer fraud claims are adequately pled.

Far from conclusory, Plaintiffs' consumer and Mass. Gen. Laws Ann. Ch. 93A, §§ 1, *et seq.* claims incorporate their detailed allegations of how Defendants' acts and practices harmed consumers. ¶¶ 4, 7, 16, 30, 123, 136, 151, 152, 189, 224-230, 237, 271, 269-71, 432-35. Moreover, as a legal matter, these claims do not, as Defendants incorrectly claim, require pleading specific misrepresentations that caused injuries to a consumer. *See Commonwealth v. Equifax, Inc.*, 2018 WL 3013918, at *4 (Mass. Super. Apr. 3, 2018). "[U]nfair trade practices which violate the FTC Act can form the basis for a private

action under Chapter 93A." *Katz v. Pershing, LLC*, 672 F.3d 64, 76 (1st Cir. 2012) (citation omitted). *See also LabMD, Inc. v. FTC*, 894 F.3d 1221, 1231 (11th Cir. 2018) ("negligent failure to design and maintain a reasonable data-security program invaded consumers' right of privacy and thus constituted an unfair act or practice" under the FTC Act).

1. Plaintiffs do not seek extraterritorial application of the ACFA, IDTPA, GBL § 349, or OCPA.

Defendants argue the ACFA, IDTPA, GBL § 349, and OCPA claims fail because these statutes do not apply extraterritorially, and there is no evidence of any event occurring within the relevant states. MTD, at 42.[28] This argument ignores the allegations in the CAC. Each claim is made on behalf of the associated state subclass,[29] who resided in the relevant states at the time of purchase and/or the Data Breach.[30] Quite simply, Plaintiffs are not looking to apply these laws extraterritorially.

2. The Illinois plaintiffs have sufficiently alleged ongoing harm.

Defendants next contend the IDTPA claim fails for lack of allegations of future harm. MTD, at 42. But it has long been recognized that economic loss is an injury. *See Transunion LLC v. Ramirez*, 141 S. Ct. 2190, 2204 (2021) ("The most obvious are traditional tangible harms, such as physical harms and monetary harms"). Here, the Illinois Plaintiffs allege they continue to pay for Defendants' services.[31] Thus, the injury from the deceptive practices (e.g., misrepresenting that Defendants would

---

[28] Defendants do not challenge Plaintiffs' Illinois Personal Information Protection Act claim (Seventeenth Claim for Relief) and the Illinois Consumer Fraud and Deceptive Practices Act (Eighteenth Claim for Relief).

[29] ¶ 383 (defining Arizona, Illinois, New York, and Oklahoma subclasses); ¶ 529 (ACFA claim on behalf of Arizona subclass); ¶ 624 (IDTPA claim on behalf of Illinois subclass); ¶ 633 (GBL § 349 claim on behalf of New York subclass); ¶ 641 (OCPA claim on behalf of Oklahoma subclass).

[30] *See, e.g.*, ¶¶ 11-12 (Doermann is New York resident who enrolled in 2018 and 2022); ¶¶ 39-40 (LeFebvre is Oklahoma resident who enrolled in 2010); ¶¶ 53-54 (Andrew is Illinois resident who enrolled in 2017); ¶ 105 (Eagleston is Arizona resident who enrolled in 2012); ¶¶ 118-19 (Shi is Illinois resident who enrolled in 2017); ¶¶ 160-61 (Klein is New York resident who enrolled in 2011 and 2012); ¶¶ 184-85 (Carter is New York resident who enrolled in 2018); ¶ 198 (Debt Cleanse's principal place of business is in Illinois, and it enrolled in 2015).

[31] *See, e.g.*, ¶ 54 (Andrew paid approximately $48 per year; no allegation this has stopped); ¶ 68 (Brook paid approximately $37 per year; no allegation this has stopped); ¶ 119 (Shi paid approximately $36 per year; no allegation this has stopped); ¶ 199 (Debt Cleanse paid approximately $120 per month; no allegation this has stopped).

protect the subclass members' PII, *see* ¶ 627.d) is ongoing; in one case as often as every month.[32] *Kurowski v. Rush Sys. for Health*, 2023 WL 2349606, at *8 (N.D. Ill. Mar. 3, 2023) ("[T]he future harm that [the plaintiff] and other similarly situated [patients of the defendant] face by continuing to use [the defendant's] web properties is sufficient at the present stage to support her claim for injunctive relief under the DTPA.").

3. What information was lost and what information was encrypted are questions of fact that the Court should not resolve at this stage.

Defendants next contend the CCRA claim fails because only certain "unencrypted customer information . . . was potentially impacted," and this information does not qualify as "personal information" under the statute. MTD, at 43. This argument is predicated on a number of factual disputes that are inappropriate to resolve at this stage of litigation. *See Lowe v. Mills*, 68 F.4th 706, 713 (1st Cir. 2023) (the Court should a complaint's "well-pleaded facts as true" and "draw all reasonable inferences in [Plaintiffs'] favor.").

First, Defendants' argument presumes they did not lose other unencrypted information. Defendants do not cite any allegation in the CAC to establish their list of information at issue, instead relying solely on their *own* exhibits. MTD, at 43. But the CAC alleges, for example, that financial information was unencrypted and lost. *See, e.g.*, ¶¶ 311, 404.a. Thus, the very presumption at the center of Defendants' argument runs contrary to the CAC. At this stage, the Court should accept the CAC's well-pled allegations as true. *Lowe*, 68 F.4th at 713.

[32] *See Asch v. Teller, Levit & Silvertrust, P.C.*, 2003 WL 22232801, at *6 (N.D. Ill. Sept. 26, 2003) ("Unlike a case where a consumer has been injured in the past and is unlikely to be injured by defendant again, plaintiffs here have an ongoing relationship with Teller, Levit as plaintiffs will continue paying their outstanding student loan debts. In light of this, the court concludes that plaintiffs have alleged facts that show a likelihood that they will be damaged in the future if defendant's conduct continues"); *see also Thomas v. Urban Partnership Bank*, 2013 WL 1788522, at *10 (N.D. Ill. Apr. 26, 2013) (finding threat of future harm "by demanding payments under the loan, and by threatening to foreclose on her property"); *Horwitz v. Wells Fargo*, 2012 WL 5862752, at *2 (N.D. Ill. Nov. 19, 2012) ("Given plaintiff's allegations that Wells collected mortgage payments to which it is not entitled and is pursuing baseless foreclosure proceeding, the Court rejects this [lack of future harm] argument").

Second, the definition of "personal information" under California Civil Code section 1798.81.5(d)(1)(A) requires that ***either*** the name or the accompanying "data element" be unencrypted.[33] And one of the "data elements" is financial information, which the CAC alleges was unencrypted. *See* Cal. Civ. Code § 1798.81.5(d)(1)(A)(iii); ¶ 404.a. Equally, to the extent the customers' last names and first names or initials were unencrypted, it does not matter if the remaining data element was encrypted; such data constitutes "personal information" under the statute.

As it is premature to determine as a matter of law—based only on the arguments of counsel in a brief—what information was or was not encrypted or lost, Defendants' motion must be denied.

4. The CCPA claims are well pled, and Plaintiffs gave the requisite notice.

Defendants first argue the CCPA claim fails because the CAC fails to allege their security was deficient and only parrots the language of the statute. MTD, at 45. But this is untrue. As discussed above, the CAC provides a great deal of detail as to what reasonable security measures Defendants failed to take. *See* Section B.1, *supra*.

Defendants also challenge the request for statutory damages on the CCPA claim on the grounds that the California Plaintiffs failed to send pre-suit notice before filing suit. MTD, at 45. Even assuming Defendants' position that Plaintiffs failed to provide adequate notice were correct (which it is not), it would at most lead to dismissal of Plaintiffs' request for statutory damages under the CCPA, not their request for any other relief on that claim. *Guy v. Convergent Outsourcing, Inc.*, 2023 WL 4637318, at *9 (W.D. Wash. July 20, 2023) (holding CCPA's pre-suit notice requirement does not apply to request for pecuniary damages).

Furthermore, Plaintiffs' notice is timely. The CCPA claim was first alleged in the CAC, which was filed on August 4, 2023, several months *after* the CCPA notice letters were sent to Defendants.

[33] "Personal information" includes "[a]n individual's first name or first initial and the individual's last name in combination with any one or more of . . . [certain identified] data elements, when either the name or the data elements are not encrypted or redacted." Cal. Civ. Code § 1798.81.5(d)(1)(A).

¶¶ 584-85, 587 (CCPA notice letters sent on January 16, 2023, February 21, 2023, and June 9, 2023). Defendants have thus been given "the opportunity afforded to [them] under the CCPA to cure the injury." *Guy*, 2023 WL 4637318, at *9. Contrary to Defendants' argument, the CCPA does not require the opportunity to cure occur prior to the filing of the original complaint. *Id.* Notably, the plaintiff in *Griffey v. Magellan Health, Inc.* (the only CCPA case cited by the Defendants) brought a claim for violation of the CCPA before providing notice. Here, in stark contrast, no CCPA claim was alleged until at least 30 days after the CCPA notice was provided. The Court should follow *Guy* in rejecting *Griffey*. *See Guy*, 2023 WL 4637318, at *9 (rejecting *Griffey* "because the court there provided no explanation as to why it dismissed the claim with prejudice or why doing so would align with the purpose of the CCPA").[34] Defendants are wrong on the facts and law and their argument for dismissal of the CCPA claim must be rejected.

CONCLUSION

Plaintiffs respectfully request that Defendants' Motion to Dismiss be denied in its entirety.[35]

[34] Plaintiff Noah Bunag first appeared as a plaintiff in the suit as part of the CAC, which was filed months after the CCPA notice letters were sent. Thus, even if, *arguendo*, the other California Plaintiffs could not seek statutory damages under the CCPA because they brought suit prior to sending the notice letters, Plaintiff Bunag does not suffer from that same infirmity.

[35] Where the Court determines it necessary to grant Defendants' Motion, Plaintiffs request leave to amend to add new details about criminal use of information obtained from the Data Breach that has come to light since filing the Complaint.

Date: October 18, 2023

Respectfully Submitted,

*Admitted *pro hac vice*

/s/ Edward F. Haber

Edward F. Haber (BBO# 215620)
Ian McLoughlin (BBO #647203)
Patrick J. Vallely (BBO# 663866)
SHAPIRO HABER & URMY LLP
One Boston Place, Suite 2600
Boston, MA 02108
Tel: (617) 439-3939
Fax: (617) 439-0134
ehaber@shulaw.com
imcloughlin@shulaw.com
pvallely@shulaw.com

Interim Liaison Counsel

Amy Keller*
James A. Ulwick*
DICELLO LEVITT LLP
Ten North Dearborn Street, Sixth Floor
Chicago, IL 60602
Tel: (312) 214-7900
Fax: (312) 253-1443
akeller@dicellolevitt.com
julwick@dicellolevitt.com

Nathaniel L. Orenstein (BBO #664513)
Patrick T. Egan (BBO #637477)
Justin N. Saif (BBO #660679)
BERMAN TABACCO
One Liberty Square
Boston, MA 02109
Tel: (617) 542-8300
Fax: (617) 542-1194
norenstein@bermantabacco.com
pegan@bermantabacco.com
jsaif@bermantabacco.com

Christina M. Sarraf**
BERMAN TABACCO
425 California Street, Suite 2300
San Francisco, CA 94104
Tel: (415) 433-3200
Fax: (415) 433-6382
csarraf@bermantabacco.com

Nicholas A. Migliaccio*
Jason Rathod*
Bryan Faubus*
MIGLIACCIO & RATHOD LLP
412 H Street NE, Ste. 302
Washington, DC 20002
Tel: (202) 470-3520
Fax: (202) 800-2730
nmigliaccio@classlawdc.com
jrathod@classlawdc.com
bfaubus@classlawdc.com
Interim Co-Lead Counsel for the Plaintiffs

Michael R. Reese*
REESE LLP
100 West 93rd Street, 16th Floor
New York, New York 10025
Tel: (212) 643-0500
Fax: (212) 253-4272
mreese@reesellp.com

George V. Granade*
REESE LLP
8484 Wilshire Boulevard, Suite 515
Los Angeles, California 90211
Tel: (310) 393-0070
Fax: (212) 253-4272
ggranade@reesellp.com

Charles D. Moore*
REESE LLP
100 South 5th Street, Suite 1900
Minneapolis, Minnesota 55402
Tel: (212) 643-0500
Fax: (212) 253-4272
cmoore@reesellp.com

Interim Co-Lead Counsel for the California Subclass

James J. Pizzirusso*
HAUSFELD LLP
888 16th Street, N.W.
Suite 300
Washington, D.C. 20006
Tel.: (202) 540-7200
Fax: (202) 540-7201
jpizzirusso@hausfeld.com

Steven M. Nathan*
HAUSFELD LLP
33 Whitehall Street
Fourteenth Floor
New York, NY 10004
Tel.: (646) 357-1100
Fax: (212) 202-4322
snathan@hausfeld.com

Thomas A. Zimmerman, Jr.*
ZIMMERMAN LAW OFFICES, P.C.
77 W. Washington St., Ste 1220
Chicago, IL 60602
Tel: (312) 767-6463
Fax: (312) 440-4180x
tom@attorneyzim.com

Chairs of the Plaintiffs' Executive Committee

Sabita J. Soneji*
Cort T. Carlson*
TYCKO & ZAVAREEI LLP
1970 Broadway, Suite 1070
Oakland, CA 94612
Tel: (510) 254-6808
Fax: (202) 973-0950
ssoneji@tzlegal.com
ccarlson@tzlegal.com

Robert C. Schubert*
Amber L. Schubert*
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union Street, Suite 200
San Francisco, CA 94123
Tel: (415) 788-4220
Fax: (415) 788-0161
rschubert@sjk.law
aschubert@sjk.law

Laura Van Note*
Cody Bolce*
COLE & VAN NOTE
555 12th Street, Suite 2100
Oakland, CA 94607
Tel: (510) 891-9800
Fax: (510) 891-7030
lvn@colevannote.com
cab@colevannote.com

Michael Kind*
KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, NV 89123
Tel: (702) 337-2322
Fax: (702) 329-5881
Email: mk@kindlaw.com

Marc E. Dann*
Brian D. Flick*
DannLaw
15000 Madison Avenue
Lakewood, OH 44107
Tel: (216) 373-0539
Fax: (216) 373-0536
notices@dannlaw.com

Francis A. Bottini, Jr.*
Albert Y. Chang*
BOTTINI & BOTTINI, INC.
7817 Ivanhoe Ave., Suite 102
La Jolla, CA 92037
Tel: (858) 914-2001
Fax: (858) 914-2002
fbottini@bottinilaw.com
achang@bottinilaw.com

Plaintiffs' Executive Committee

Counsel for the Plaintiffs

CERTIFICATE OF SERVICE

I, Edward F. Haber, hereby certify that I caused a copy of the foregoing document to be filed electronically via the Court's electronic filing system. Those attorneys who are registered with the Court's electronic filing system may access this filing through the Court's system, and notice of this filing will be sent to these parties by operation of the Court's electronic filing system.

Dated: October 18, 2023

/s/ Edward F. Haber
Edward F. Haber